EXHIBIT 1

Rackspace G-Cloud Government Cloud on VMware (RGC-V) Terms and Conditions

rackspace technology®

RACKSPACE GOVERNMENT CLOUD ON VMWARE PRODUCT TERMS

In addition to any other terms and conditions of Client's Agreement with Rackspace, these Product Terms apply where Client purchases Rackspace Government Cloud on VMware Services. Any amounts in US$ are equivalents in local currency, as determined by Rackspace, if invoiced in local currency.

These Product Terms are subject to and governed by the Rackspace Master Services Agreement ("MSA") found at https://www.rackspace.com/information/legal/msa.

1. ADDITIONAL DEFINED TERMS.

"**A&A Package**" means the Assessment and Authorization set of documents, consisting of the System Security Plan, supporting security plans, test results, plan of action, and milestones.

"**Available Hours**" means the total number of hours in an applicable month less the number of Cloud Infrastructure downtime hours attributable to Scheduled Maintenance and Emergency Maintenance in the same month.

"**Actual Uptime**" means applicable monthly Available Hours less Client Cloud Infrastructure downtime hours attributable to causes other than Scheduled Maintenance and Emergency Maintenance in the same month.

"**Border Routers**" means any routers that connect Rackspace's internal network to a transit or peering provider via Border Gateway Protocol (BGP). The external WAN interface uplinking the router to a third-party fiber or cross-connect provider is not included in this definition.

"**Business Hours**" means, for the sake of these Product Terms, 9:00 AM to 5:00 PM (Eastern Standard Time within the US, and Coordinated Universal Time within the UK), on Business Days.

"**Compliance Baseline**" means the defined set of security controls to which the Services are managed, as specified in the Service Order.

"**Contingency Plan**" means the artifact of the Compliance Baseline A&A Package required by all Cloud Service Providers. It denotes interim measures to recover information system services following an unprecedented emergency or system disruption. The Rackspace Contingency Plan is internal to Rackspace.

"**Client Access Switch**" means the Rackspace-managed access switch uplinked to the Production Environment.

"Client Appliance" means any Client-owned and managed virtual machine (VM).

"**Client Portal**" means Rackspace's Client ticketing and/or notification portal.

"**Cloud Infrastructure**" means the hardware and software resources, which are located in enterprise-grade data centers, used to deploy the Services, including the host servers, switches, firewalls, hypervisor, and Operating System Instances (OSIs) provided by Rackspace, as set forth in Client's Service Order(s). This excludes Client Appliances.

"**Disaster Declaration**" means the submission by the authorized Client representative of a ticket, via the ticketing method designated by Rackspace, declaring a disaster event and requesting that Rackspace initiate a restoration of the Production Environment at its Disaster Recovery Site.

"**Disaster Recovery Site**" means the secondary site where Client production data will be replicated.

"**Disaster Recovery Testing**" means verifying the processes and services in place through simulated recovery of a mutually agreed-upon portion of the Production Environment in the Disaster Recovery Site.

"**Emergency Maintenance**" means any critical unforeseen maintenance or upgrades needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"**Minimum Level Resources**" means the committed minimum capacities for each resource used to provide the Services specified in the Service Order(s).

"**Monthly Services Fee**" means those monthly fees incurred by Client that are related to the Services provided by Rackspace under these Product Terms.

"**Operating System Instance (OSI)**" means an independent, functional virtual or bare metal server running an operating system that is both supported by the operating system manufacturer and offered by Rackspace. This excludes Client Appliances.

"**Parties**" means Rackspace and Client collectively. "**Party**" means Rackspace or Client individually.

"**Production Environment**" means the total Client environment, encompassing the entirety of contracted Services being delivered to Client in support of Client's production cloud solution, but explicitly excludes any resources designated "non-production" and/or "dev/test". This is inclusive of Cloud Infrastructure, Client Appliances, OSIs, Compliance Baseline, and any optional Services as provided by Rackspace and set forth in Service Order(s).

"**Privileged User**" means any user of the Client environment with access authority greater than users of the environment's applications. Privileged Users include application, database, network, system, and security administrators.

"**Recovery Point Objective**" or **"RPO"** means the maximum period of permitted data loss upon Restoration Success, measured in hours preceding the time of failure.

"**Recovery Time Objective**" or "**RTO**" means the duration of time, measured in hours, between Rackspace confirmation of a Disaster Declaration and Restoration Success.

"**Restoration Success**" means that the Operating System Instances at the Disaster Recovery Site are online and available for Client to use.

"**Rackspace Equipment**" means the Rackspace hardware used to provide the Services as set forth in these Product Terms.

"**Rackspace Network**" means the internal LAN-side Ethernet interface of the Border Routers to the Client Access Switch via all Rackspace-owned and -managed networking hardware.

"**Rackspace Support**" means the 24 hours a day, seven days a week, year-round support made available by Rackspace via the ticketing method designated by Rackspace or by phone (at 866 522 0070 in the US or 0333 003 4000 in the UK, or such other phone number as Rackspace may designate in the future).

"**Scheduled Maintenance**" means any planned maintenance or upgrades (including tech refreshes) needed for the security, redundancy, or performance of the Production Environment, Rackspace infrastructure, and/or the Rackspace Network.

"**Solution Escalation Action Plan (SEAP)**" means the jointly-prepared Client management plan that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts. Specific monitoring thresholds are also documented in the SEAP.

"**System Security Plan**" means the main document of the A&A Package detailing how a Cloud Service Provider manages the security controls throughout the lifecycle of the Services, in accordance with the Compliance Baseline.

In addition to the narrative of the security control implementation, it also includes a system description of the components and services inventory, and depictions of the system's data flows and authorization boundary.

"**vCore**" means a unit of server compute resources.

2. EXPORT MATTERS. Client may not provide access to the Services to any person (including any natural person, government, or private entity) that is located in, or is a national of, any country that is embargoed or highly restricted under applicable export laws and regulations.

3. SERVICE INFORMATION. Rackspace provides a fully managed cloud platform designed to support government cloud workloads. The Services are designed with single-tenant server, storage, and networking hardware managed 24x7 by Rackspace's operations teams. Rackspace is responsible for implementing and managing the Production Environment, up through and including the hypervisor for Client-provided Appliances and the OSI layer for all other Client VMs. Rackspace shall upgrade the Cloud Infrastructure as reasonably necessary to comply with the terms of the Agreement. The Services include implementation and ongoing management of the Compliance Baseline. At a minimum, the Compliance Baseline implements either a subset of the NIST SP 800-53 Revision 4 Moderate impact security controls, or NCSC's 14 Cloud Security Principles (where applicable) but may include additional overlays and/or Client-defined controls. Any controls in addition to, or in lieu of, provisionally authorized controls may be mutually agreed upon and included, provided there is no conflict of applicable laws, Executive Orders, directives, policies, regulations, or other mandated compliance requirements. Any additional, mutually agreed-upon controls shall be identified and set forth in the applicable Service Order, inclusive of any additional implementation and management fees, prior to being implemented and provided as part of the Services.

3.1. Managed Cloud Infrastructure Services.

(A) System Administration & Maintenance Services. Rackspace provides system administration and maintenance services for all elements of the Services. Compute, storage, network, and OSIs are configured, hardened, and managed per pre-defined configuration management controls. Rackspace installs and implements Client's Production Environment; and provides the maintenance, repair or replacement of all Cloud Infrastructure components of Client's environment. Client is solely responsible for all administration, maintenance, security, and compliance management services required for any software or program installed on the Rackspace-provided and -managed OSIs. Rackspace shall attempt to schedule maintenance for a time that minimizes impact on Client, and shall provide notice of Scheduled Maintenance.

(B) Cloud Server Compute Resources. Rackspace provides the use of dedicated computing resources as vCores to support Client's applications. Each increment of vCore includes computing resources of up to 4GB of memory and one virtual CPU Core that can be combined to create virtual machines to match Client's requirements (e.g., combining multiple vCore resources to create a dual core virtual CPU, 8GB RAM virtual machine).

(C) Cloud Storage Services. Rackspace provides a fully managed storage environment for OSIs, Client Appliances, backups, and disaster recovery, separated at the Client tenant level. Storage options are tiered for price and performance optimization, and provisioned and billed in 100GB increments, as defined in the Service Order.

(D) Capacity Planning. Client may request alerts when pre-defined thresholds (documented in the SEAP) have been reached. These alerts shall proactively notify Client that additional resources may be required to support their workloads. All requests for additional resources shall be made in writing, either via the ticketing method designated by Rackspace or executed Service Order.

(E) Network Services. Rackspace provides highly available LAN configurations as well as redundant WAN connectivity through multiple Tier I internet service providers, including Rackspace Network links between data centers. Rackspace shall provide availability monitoring of all Rackspace Network components. Rackspace also implements denial-of-service (DoS) protection mechanisms at the network ingress and egress points

(F) Network Capacity. Rackspace limits public internet bandwidth to a maximum of 5 Mbps per OSI. Additional bandwidth usage shall incur additional charge.

(G) Infrastructure Services Specifications.

SERVICE AREA	RACKSPACE STANDARD OFFERING
Bandwidth	Rackspace provides: • 10 Gbps connectivity at the primary and secondary data centers. • 10 Gbps Rackspace Network connection for replication between the primary and secondary data centers. • Firewall at ingress/egress

(H) OSI Management. Rackspace shall provide provisioning, hardening, encryption, administration, backups, monitoring, and alerting of the Production Environment OSIs deployed, as set forth in this Section 3.1(G) and in the applicable Service Order.

(i) Provisioning. The Rackspace Cloud Server Management Implementation Service provides the implementation and initial testing of the monitoring, alerting, and O/S administration tools for the cloud servers deployed.

(ii) Hardening. Rackspace hardens OSIs (Red Hat Enterprise Linux and Microsoft Windows Server only) and network devices to its configuration baseline based on Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) benchmarks. Prior to Client environment deployment and configuration, Rackspace shall communicate the STIG benchmark version to be implemented and managed. Any Client-defined hardening requirements in addition to, or in lieu of, the Rackspace DISA STIG configuration baseline shall be identified and set forth in Services Order(s), inclusive of any additional implementation and management fees, prior to being implemented and provided as part of the Services.

(iii) Encryption. Rackspace manages transparent FIPS 140-2 validated encryption at the storage layer. Compliance Baseline encryption requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Client.

(iv) Administration. Rackspace provides administration of OSIs, including routine preventative maintenance, monthly patching, and troubleshooting, and may include additional services, as defined in the Service Order.

(v) Backups. Rackspace performs image-based Changed Block Tracking backups of Production Environment OSIs and Client Appliances once per day. If file-level, database-level, or otherwise application-aware backups are required, Client is responsible for providing a compatible backup solution – e.g., database-native backup to a local disk included in the daily image backup. Unless otherwise specified in the Service Order, the backups for Production Environment OSIs and Client Appliances shall be available onsite for 14 calendar days, and the Production Environment backups shall be replicated from the primary backup location to the archival backup location available in the Disaster Recovery Site for the same 14-day period. Client may request additional Services for longer retention periods, as defined in the Service Order. Any required restores shall only be created from Rackspace-provided disk images and presented to the OSI as a full disk. Client may choose to replace the existing disk or mount as an additional disk; but all file-level, application or database recovery efforts are Client's responsibility.

(I) Managed Security and Compliance Services. Rackspace performs the following functions, in accordance with the Compliance Baseline, to secure the Rackspace Network and Cloud Infrastructure.

Compliance Baseline requirements for any software or program installed on top of the Rackspace-provided and -managed OSIs are the sole responsibility of Client.

(i) 24x7 Monitoring and Alerting. Rackspace monitors the performance, availability, and network connectivity of supported cloud servers 24x7. By default, all alerts are configured to go to Rackspace, but the SEAP can be updated to define Client notification and escalation criteria.

(ii) Access Control (AC). Rackspace's architecture and processes maintain controlled Privileged User access to the Cloud Infrastructure. Privileged Users shall access the Cloud Infrastructure with an encrypted VPN connection established using multi-factor authentication. This connection from outside the environment can only be made to an approved jump host server. While the connection is in place, all other internet communication from the Privileged User's source device is disabled. From the jump host, privileged users can access other devices within the Cloud Infrastructure via Remote Desktop Services or SSH based on role privileges set up by Rackspace.

All privileged user sessions on jump hosts are recorded to provide a detailed activity log to support potential security incident analysis and response.

Rackspace shall be responsible for and have administrator control over the domain, forest, and/or organizational units that comprise the computer, user, and service accounts that pertain to, and provide access to, the Production Environment.

(iii) Awareness and Training (AT). All Rackspace engineering staff supporting the Cloud Infrastructure receive annual privacy and information security awareness training.

(iv) Audit and Accountability (AU). This Section 3.1(I)(iv) applies solely to Services provided within the United States.

Rackspace configures all elements of the Cloud Infrastructure to feed audit information into a centralized logging platform that provides near-real-time log collection, indexing, and management separated at the Client tenant level for: (i) System Security logs, (ii) IDS logs and (iii) Firewall logs.

Rackspace's centralized logging platform allows Rackspace security engineers and analysts to use a suite of automated and manual tools to extract audit information. In the event of a security incident or suspected incident, logs assist in determining: (i) if there was an incident, (ii) who was involved in the incident, (iii) when the incident took place, (iv) what type of incident took place and (v) how the incident occurred.

Logs are collected and retained online for 90 days through replication to the online log server and further preserved offline for one year.

Client is responsible for retaining application and database audit records online, in order to provide support for after-the-fact investigations of security incidents and to meet their respective regulatory and organizational information retention requirements. Client may purchase additional Services to store their logs. Client retains all responsibility for configuration and management of these additional log sources.

(v) Configuration Management (CM). Rackspace uses a baseline configuration based on DISA STIGs. Rackspace follows change and configuration management procedures detailed in the Configuration Management Plan as part of the A&A Package. As part of Rackspace's configuration management process, all proposed changes are recorded and analyzed for impact, and any Client-impacting changes are coordinated with Client. In addition, where Rackspace has responsibility for managing customer Active Directory, configuration tools automatically develop baselines when initially configured, and maintain those baselines by comparing any changes to the baseline, at least once per quarter, as the system is being used.

Any Client-defined hardening other than the Rackspace-defined configuration baseline shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(vi) Quarterly Configuration Compliance Scanning and Reporting. Rackspace scans the managed OSIs for compliance with the Rackspace-defined hardening configuration standard. The raw, unmodified compliance scan results shall be provided quarterly to Client for each environment.

Any Client-defined hardening configurations, other than the Rackspace-defined configuration baseline, shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

Any custom-configuration compliance scanning and associated reporting shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

(vii) Contingency Planning (CP). Rackspace maintains a Contingency Plan for the Rackspace Cloud Infrastructure as required by Compliance Baseline requirements. Rackspace shall support Client Contingency Planning efforts by meeting the Recovery Point Objective and Recovery Time Objective in the event of a major disruption to the Production Environment. The SEAP shall be used to define the tools, processes, and procedures within the areas of responsibility of Rackspace and Client. Rackspace shall provide one Disaster Recovery Test per year, upon Client request with written notice 30 days prior. This can include turning on virtual machines at a secondary facility; running specific workloads at a secondary facility in a temporary, non-impactful way; verifying data backup integrity; or testing for hardware outages.

(viii) Disaster Recovery. Rackspace provides replication of Client Production Environment OSIs and Client Appliances to a Disaster Recovery Site. Rackspace manages the Disaster Recovery Site and provides disaster recovery support services in accordance with the SEAP. Upon a Disaster Declaration, replicated VMs are activated by Rackspace in the Disaster Recovery Site to seek to restore Services to support Restoration Success within the RPO and RTO. RTO does not include any third-party dependencies outside of Rackspace's control, including Client application coming back online and time required for external third-party components and network protocols to be migrated by third-party providers. Any other application-level activities to recover and reconstitute the Client Production Environment are the responsibility of Client.

Rackspace makes no warranty as to the quality, contents or formatting of Client data. Client accepts and acknowledges the limitations of data replication, specifically that data corruption and deletion within the Production Environment, both intentional and unintentional, will be replicated to the Disaster Recovery Site. As such, Disaster Recovery shall NOT be used as a replacement for application state and database backups, which remain the sole responsibility of Client. Additionally, the rate at which the data in the Production Environment can be transferred to the Disaster Recovery Site shall vary depending on the rate of change, amount and type of data, constraints inherent in the Services, and fluctuations in bandwidth availability. Therefore, at any given time, the Disaster Recovery Site may not be completely up to date. In the event of a failover to the Disaster Recovery Site, data that has not yet completed transfer from the Production Environment shall be lost commensurate with the Recovery Point Objective. Client also accepts and acknowledges that this same risk of data loss exists during execution of Disaster Recovery Testing. Rackspace is not liable for any data loss as a result of performing Client initiated Disaster Recovery Testing, nor by executing Client's instructions in the event of a legitimate Disaster Declaration.

The Disaster Recovery Services provided are not a full business continuity solution. It is intended to be a component in a Client managed and executed business continuity plan. As such, Rackspace takes no responsibility for, and does not guarantee, any business continuity capabilities as a result of Client's use of the Disaster Recovery Services.

Where Client has not purchased VM Replication Enhanced Edition for Government Services the services shall enable the ability to meet an RPO and RTO commensurate with the Compliance Baseline; and unless otherwise specified in a Service Order the default RPO and RTO are both 24 hours.

Solely where Client purchases VM Replication Enhanced Edition for Government Services, and both the Client Production Environment and Disaster Recovery Site are located in the same country, then RPOs and RTOs shall not be set commensurate with the Compliance Baseline, and instead shall enable the ability to meet a RPO and RTO commensurate with commensurate with the Disaster Recovery Tier identified in the Service Order(s), as set out below:

Disaster Recovery Tier	RPO & RTO
Bronze	24 Hours
Silver	12 Hours
Gold	4 Hours
Platinum	1 Hour

Alternatively, Client can opt to deploy their Production Environments in an active-active manner, in which the Production Environment can always be running in the Disaster Recovery Site as well. Active-active configuration is a Client responsibility, outside of the scope of the base Services configuration, and would typically require application-level support.

(ix) Identification and Authentication (IA). This Section 3.1(I)(ix) applies solely to Services provided within the United States. Rackspace provides a Client-specific identity store implemented via Active Directory domain. This Active Directory domain resides on a pair of highly available domain controllers within the Production Environment. All resources within the Production Environment are domain-joined, including the VPN concentrator, which requires multi-factor authentication to establish a tunnel. This tunnel only exposes a single jump host, which is also domain- joined.

(x) Maintenance (MA). Rackspace shall coordinate maintenance windows to perform Scheduled Maintenance activities as required for the Cloud Infrastructure components that Rackspace supports. Rackspace shall notify Client of Scheduled Maintenance at least five Business Days before maintenance is scheduled to occur. Scheduled Maintenance may be adjusted by Rackspace up to 24 hours in either direction (before or after the then-current maintenance schedule); however, to the extent Client requires changes to the maintenance schedule, Client shall coordinate such change within 24 hours of Rackspace notification.

On occasion, Emergency Maintenance may be required to maintain a security posture commensurate with the Compliance Baseline. Rackspace is authorized to perform all reasonable actions to meet or exceed requirements in connection with the delivery of the Services against the Compliance Baseline. Rackspace shall make every effort to provide advanced notification to Clients whenever possible, but specific circumstances may dictate immediate action without prior notification.

(xi) Media Protection (MP). Rackspace utilizes validated cryptographic mechanisms to encrypt removable storage media within Rackspace data centers. All physical media transport outside of the data center is strictly controlled. Unless set forth in a separate agreement, Rackspace shall not accept any Client-furnished storage devices, and Rackspace shall not provide to Client any Rackspace storage devices. All decommissioned disk drives and digital media are sanitized before any physical destruction, in accordance with the Compliance Baseline. Physical destruction of disks may incur an additional charge.

(xii) Personnel Security (PS). All Rackspace personnel with physical or logical access to the Cloud Infrastructure shall be resident citizens of the US and/or UK, commensurate with the Compliance Baseline requirements, and undergo pre-employment background checks as part of the on-boarding and application process. An employee's hiring is contingent upon internal investigations, such as background, credit, and reference checks.

If Client requires personnel security approvals or clearances outside of Rackspace's standard background investigation, then Rackspace reserves the right to submit for approval and/or clearance its entire operations and security teams associated with the Services to enable adequate support. Client shall bear the costs and expenses incurred by Rackspace in connection with obtaining approvals or clearances required to allow Rackspace to perform its obligations hereunder.

(xiii) Physical Environment (PE). Rackspace data centers implement security safeguards to control access to areas within the facility that are officially designated as publicly accessible. Rackspace uses badges for all personnel with access privileges. Rackspace maintains a current list of personnel with authorized access to the areas where the Cloud Infrastructure resides, in addition to maintaining a separate list of personnel with authorized access to the government-only enclave area. The data center floor incorporates badge and biometric access controls, alarmed dual-factor authenticated locked doors, CCTV, and 24x7 guards to enforce physical access authorizations at all access points. Separate controlled access is required to access a government-only enclave area of the data center.

(xiv) Risk Assessment (RA).

(a) Monthly Vulnerability Scanning. Rackspace performs monthly vulnerability scanning for each Client's managed OSIs within their environment(s). The scans are performed by Rackspace and the raw, unmodified vulnerability scan results shall be provided to Client. Rackspace and Client shall mutually agree on a monthly scanning schedule for the duration of the services agreement.

Any custom vulnerability scanning activities and associated reporting requested by Clients shall be stated in any applicable Service Order(s), which shall include additional implementation and management fees.

Client's security obligations include immediately remediating any known security vulnerability of any Client Appliance, or any software or program installed on top of the Rackspace provided and managed hardware and software Services.

(xv) System and Communication Protection (SC). Rackspace separates user functionality from management functionality through physical and logical network segmentation and associated access management policies. The Cloud Infrastructure is separated into at least two security environments: 1) a management environment containing Rackspace's support tools, and 2) Client's Production Environment. Client may implement "non-production" environments. Access to each environment is controlled by a logical firewall. Access to the management environment is limited to only Rackspace personnel. Privileged Users access the Production Environment using multi-factor authentication into a jump host via an encrypted VPN connection. End users of Client's application enter through Client-managed, application-defined mechanisms.

Rackspace provides each Client environment with a network intrusion detection sensor that monitors all network traffic to and from the Client's Production Environment. The sensor monitors all unencrypted traffic for indicators of known potential attacks and potentially malicious traffic, excluding network traffic that is encrypted using transport-layer encryption methods (e.g. HTTPS, SSL, TLS, SSH) which the sensor is unable to decrypt.

(a) System Availability. Appliance availability and failover is accomplished via component resiliency at several levels. At the network level, WAN internet connectivity is delivered through Tier 1 internet service providers. The connectivity is available via Border Gateway Protocol (BGP), whereby Rackspace announces paths for public IPs amongst all carriers. In the event of a carrier, link, or device failure, traffic is automatically re-routed.

From the edge WAN routers through to the host servers, all network devices and paths are redundantly meshed to prevent perceptible downtime in the event of the failure of any single device. Each host server has redundant path connections to both storage and production networks.

Unless otherwise specified in a Service Order, the host servers powering the Production Environment are configured in an N+1 configuration featuring VMware's high availability (HA) capability which shall restart any VM(s) from a failed host server on the remaining server nodes in the cluster.

(xvi) System Integrity (SI).

(a) Endpoint Security Management. Rackspace provides a centrally managed endpoint security software platform for all Client OSIs within their environment. The endpoint security management solution provides centralized anti-virus, malware defense**,** and host-based intrusion prevention services. Rackspace provides ongoing management of the management servers**;** agents installed on OSIs**;** and associated configurations, updates**,** and policy management. In the event a security event is detected, Rackspace shall notify and collaborate with Client to determine the appropriate actions.

(b) File Integrity Monitoring. This Section 3.1(I)(b)(ix) applies solely to Services provided within the United States, unless otherwise stated to the contrary in the Service Order. Rackspace provides a centrally managed File Integrity Monitoring (FIM) solution that monitors all Client OSIs for file changes. The FIM solution monitors core OSI operating system files and identifies and reports on changes made to these files. Monitoring the integrity of Client data and/or application files installed by Client on OSIs is excluded from the Rackspace FIM solution monitoring scope of services. Rackspace provides ongoing management of the FIM management servers; agents installed on OSIs; and associated configurations, updates, and policy management. In the event a FIM event is detected, Rackspace shall notify Client and shall collaborate with Client to determine the appropriate actions.

(xvii) Relocation. Rackspace may move or relocate Client's Production Environment and disaster recovery Services within or between data center locations (located in the same country as the origin data center). Additionally, Rackspace may make changes to the provision of the Services (including, but not limited to, changing the assigned IP addresses and DNS records and zones on Rackspace operated or managed DNS servers as Rackspace deems necessary for the operation of the shared network infrastructure).

4. AUDIT SUPPORT SERVICES. Upon at least 30 days of advance written notice, Rackspace provides up to 60 hours of security audit services for one security audit, per each 12-month period for each separate engagement following the Commencement Date of the applicable Service Order. Any additional security audit services required by Client for each Project above this time cap, shall be available during Business Hours for US$250 per person, per hour, if booked two or more weeks in advance. For less than two weeks of advance notice, additional security audit services shall be available during Business Hours for US$350.00 per person, per hour. Additional security audit services requested outside of Business Hours are available for US$450 per person, per hour. If the security audit is performed on behalf of an end client of Client, Client shall give Rackspace direct access to the end client and its auditors.

5. INCIDENT RESPONSE.

5.1. Communication During Incident Management. Client shall assist Rackspace in developing a SEAP that shall define the steps to be taken by Rackspace personnel when responding to incidents, tickets, and alerts.

During the incident management process, Rackspace and Client shall communicate via means designated in the SEAP. Communications shall be made based on the timelines defined in the SLAs listed in Section 6.

In the event that incident resolution requires Client cooperation, such cooperation shall not be unreasonably withheld.

Upon incident receipt notification by phone call or Client Portal, Rackspace shall respond to Client via the ticketing method designated by Rackspace or phone call.

Rackspace shall use commercially reasonable efforts to provide the post-incident Client incident report within two Business Days via email.

Client shall designate a primary point of contact to communicate with Rackspace regarding all technical issues that may arise during the term of any Service Orders in the agreement, including highlighting the priority and urgency of Client tickets and requests.

5.2. Support Requests. Client shall create a ticket using the method designated by Rackspace for all support requests, change requests, or incidents. Following the submission of the ticket, Rackspace's response time shall match the agreed-upon severity of the ticket, as described in Section 6.1.

Rackspace shall send an email notification to the requestor/creator of the ticket as well as the approver when a ticket is closed by Rackspace Support personnel.

5.3. Security Incident Response. In the event of a security incident in the Client Infrastructure, such as a denial of service attack, Rackspace reserves the right to suspend Services without notice as necessary (e.g., powering off or network-isolating Client Appliances and OSIs), until completion of remediation.

6. SERVICE LEVEL AGREEMENTS (SLA).

6.1. Initial Incident Response Time SLAs.

Ticket Severity	Severity Definition	Initial Response Time
Sev1	The total outage of service or availability of network connectivity (internet or internal), or mission-critical application availability, such that Client cannot continue to operate its business due to the severity of the outage.	15 minutes
Sev2	Either of the following: (i) A material degradation of service or availability of network connectivity (internet or internal), or network device failure, mission-critical application availability, or production hardware components, such that Client can continue operating its business, but in a negatively impacted and degraded mode; or (ii) Any other support request not meeting the definition of Severity Level 1.	60 minutes

Client is entitled to a credit of US$250 or the failure of Rackspace to meet the Section 6.1 Initial Response Time SLAs. The Initial Response Time begins upon the Rackspace system timestamp for submission of a ticket, resulting from a ticket being submitted by either (i) Client or (ii) Rackspace Support through the Rackspace Support phone number.

6.2. Availability SLAs. Rackspace guarantees 99.95% availability for Cloud Infrastructure. Client shall be entitled to prorated monthly Fees for each full or partial hour of downtime in excess of the Availability SLA.

6.3. Disaster Recovery SLA. Solely where Client purchases VM Replication Enhanced Edition for Government Services, Rackspace guarantees that it shall meet the applicable RTO for the Disaster Recovery Tier.). Rackspace makes no guarantee the RTO shall be achieved where the Client does not purchase VM Replication Enhanced Edition for Government Services; and in all circumstances Rackspace makes no guarantee that the RPO shall be achieved. Client is entitled to a credit of US$250 for the failure of Rackspace to meet the Section 6.3 Enhanced Disaster Recovery Time SLA.

6.4. Exceptions to the Credit Process. Credit shall not be issued due to failures that are, as determined by Rackspace, in its good faith reasonable judgment, the result of:

(A) Scheduled Maintenance or Emergency Maintenance

(B) Written agreement between Rackspace and Client confirming a change may be implemented without following the Change Control Processes

(C) Client-initiated work independently generated by Client

(D) Client support requests not submitted through a method designated by Rackspace

(E) Service interruptions requested by Client

(F) Violations of Rackspace's Acceptable Use Policy as may be updated from time to time at www.rackspace.com/information/legal/aup.php

(G) Client-required OSI revisions and hardware/software configurations that are not Rackspace tested/approved

(H) Client-created rules, objects, functional configuration errors, third-party software configuration, or other failure of Client Appliances, software, or hardware, or third-party software or hardware

(I) Events of Force Majeure

(J) DNS issues outside the direct control of Rackspace

(K) Patches or antivirus updates which contain code faults, flaws, or other errors attributable to the third-party vendors that created such code

(L) Any suspension of the Services pursuant to the terms of the Agreement

(M) A DoS attack or distributed denial-of-service attack (DDoS attack)

(N) Any actions or inactions of Client, an end user, or any third party

(O) Client's equipment, software, or other technology and/or third-party equipment, software, or other technology (other than third-party equipment within Rackspace's direct control)

(P) Client's failure to request SLA credits within 30 days of the applicable month for which Services are invoiced

(Q) Manufacturer or safety code-related shutdowns required for safety compliance

6.5. Service Level Credit Limitations. The SLA credit remedies contained in this Section are Rackspace's sole and exclusive liability and Client's sole and exclusive remedy for any failure of Rackspace to meet an SLA. Client must request SLA credits within 30 days of the applicable month for which Services are invoiced. The total credit available to Client for all SLA failures in any particular calendar month shall in no event exceed the Monthly Service Fee for the environment in which the SLA failure occurred during that invoiced month. Any credits available to Client shall be applied to Fees due from Client for the Monthly Services Fee and shall not be paid to Client as a refund, unless such credit pertains to the last month of Client's service.